UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/598,777	06/16/2000	Steven H. McCown	00-022-MIS	5604

7590 03/11/2005

Wayne P Bailey
Storage Technology Corporation
One StorageTek Drive
Louisville, CO 80028-4309

EXAMINER	
REAGAN, JAMES A	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 03/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/598,777	MCCOWN ET AL.	
	Examiner	Art Unit	
	James A. Reagan	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in reply to the amendment and response filed on 21 January 2005.

2. Claims 7, 13, 18, 19, 23, 30, 32, 37, and 38 have been amended.

3. Claims 1-40 have been examined.

4. The rejections of claims 1-40 have not been altered.

RESPONSE TO ARGUMENTS

5. Applicant's arguments received on 21 January 2005 have been fully considered but they are not persuasive. Referring to the previous Office action, Examiner has cited relevant portions of the references as a means to illustrate the systems as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first Office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims, except as noted above in the section labeled "Status of Claims." This information is intended to assist in illuminating the teachings of the references while providing evidence that establishes further support for the rejections of the claims.

6. With regard to the limitations of claim 1, it appears as if the Applicant is attacking the references in a piecewise fashion, instead of in combination, as intended by the Examiner and as shown below in the rejections under 35 USC § 103(a). Applicant argues an inconsistency regarding the phrase "Master key" in the rejections below. Although Muftic does disclose hashing a message digest as well as key utilization, Muftic does not specifically disclose a master key *per se*, hashing a master key with customer information, and the inherent transactional steps associated with a smart card transaction. Therefore, the Examiner has relied upon excerpts

from the background of the specification in combination with Muftic to fully disclose this limitation. Applicant also argues an inconsistency regarding the phrase "hashing a master key with customer information." In this case, the Examiner has relied upon excerpts from the background of the specification in combination with Muftic/Rankl to fully disclose this limitation.

Applicant asserts that Muftic *does not disclose a master key.* The Examiner respectfully disagrees and points to the Abstract and other relevant text wherein Muftic discloses Public Key Infrastructure, clearly within the bounds of the definition demanded by the Applicant on page 18, paragraph ii (a) of the response.

Applicant asserts that *none of the cited references teach or suggest the claimed step of creating a digest by hashing unique client information with the master key.* The Examiner respectfully disagrees and points to the rejection below, wherein Rankl clearly discloses hashing consumer data with the smart card unique key (see at least section 4.3 and Figure 4.23).

Applicant asserts that *none of the cited references teach or suggest the claimed step of returning the digest and the unique client information to the requestor.* However, Muftic discloses that when using hashes, the method for determining if a message is authentic is by doing a similar hash and comparing the results (C2, L27-37). Moreover, Muftic clearly teaches that the way to authenticate a hashed message is by using the same components, doing a parallel hash, and comparing the results. It is plainly obvious that in order to perform a proper validation and authorization of a transaction, the authorizing entity must inherently perform a parallel hashing of merchant, client, transaction IDs, and matching master key, and then compare the resulting digest with the one received from a requestor, in order to determine whether the request may be authorized.

With regard to the limitations of claim 2, Applicant asserts that *none of the cited references teach or suggest the claimed step of the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information.*

The Examiner respectfully disagrees. A seller ID is a unique Identifier easily incorporated into the hashing algorithm that uniquely identifies a transaction between a buyer and a seller. As is known in the art, the ID could be a simple as an email address of a variable string of characters. As shown above, However, Muftic discloses that when using hashes, the method for determining if a message is authentic is by doing a similar hash and comparing the results (C2, L27-37). Moreover, Muftic clearly teaches that the way to authenticate a hashed message is by using the same components, doing a parallel hash, and comparing the results. It is plainly obvious that in order to perform a proper validation and authorization of a transaction, the authorizing entity must inherently perform a parallel hashing of merchant, client, transaction IDs, and matching master key, and then compare the resulting digest with the one received from a requestor, in order to determine whether the request may be authorized.

With regard to the limitations of claim 3, Applicant asserts that *none of the cited references teach or suggest the claimed step of the request includes unique merchant information which is used to access the master key.* However, as shown above, a seller ID is a unique identifier easily incorporated into the hashing algorithm that uniquely identifies a transaction between a buyer and a seller. In addition, the Examiner states that Seller IDs are an inherent *part* of the credit card system, clearly in support of the rejection under 35 U.S.C. 103(a). In addition, Muftic does disclose providing a token or certificate (i.e. "master key") assigned to a unique client account, clearly indicating singular access by only authorized entities to privileged information.

With regard to the limitations of claim 5, Applicant argues against the Examiner's rationale for the Muftic citation against the limitations. However, as is plainly known to one of even basic skill in computing arts, smart cards a miniature computers with microprocessors, easily capable of running HASH algorithms, as the prior art of references shows. In this case, the Examiner has pointed out particular references contained in the prior art of record within the body

of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

With regard to the limitations of claim 6, any one of ordinary skill in the art of computer security understands that encrypting a document after it has arrived at its destination without encrypting it for the duration of the transmission would be repugnant to the intent of encrypting the data in the first place.

With regard to the limitations of claim 7, it appears as if the Applicant is reading limitations into the claim that are not recited in the claim as written. Arguments are therefore moot. Elements regarding claim 2 are addressed above.

With regard to the limitations of claims 8 and 10-12, see the passage regarding claim 1 above. Also, utilization and transmission of unique identifiers is intrinsic to a unique transaction.

With regard to the limitations of claims 13-19, see the Examiner's remarks regarding claims 1 and 8 above.

With regard to the limitations of claim 20, the Examiner respectfully disagrees and points to the passages above regarding claims 1 and 8 as well as the rejections below.

With regard to the limitations of claim 2-40, the Examiner respectfully disagrees and points to the passages above regarding claims 1 and 8 as well as the rejections below.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-3, 5-8, 10-14, 17-26, 28-33, and 36-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic, (US 5,850,442 A), in view of the Applicant's own admissions, and further in view of Rankl, (Smart Card Handbook (c) 1997).

Examiner's Note: The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Claim 1:

Muftic, as shown, discloses the following limitations:

- *receiving, prior to the transaction, a secret master key from a third party, wherein the master key remains unchanged and is kept secret and is not altered after the transaction, the third party storing a copy of the master key*

(see at least Abstract, Summary of the Invention, Fig 16: "smart token/certificate", associated text);

- *receiving a request for a digest from a requestor* (see at least C2, L27-51: "message digest"; Fig 10: step 1030: "receive order form"; associated text);
- *retrieving the master key* (retrieving unique client information (see at least Fig 10: step 1060: "digitally sign order form"; Fig 10, steps 1040, 1060);
- *the client information being associated with the master key* (see at least Fig 10: step 1060);
- *creating the digest by hashing the unique client information and the master key* (see at least C2, L38-41);
- *returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with a third party* (see at least Fig 10: step 1060).

Although Muftic does disclose hashing a message digest as well as key utilization, Muftic does not specifically disclose a master key *per se*, hashing a master key with customer information, and the inherent transactional steps associated with a smart card transaction. Applicant, however, in at least page 19, lines 24-25, and on page 21, lines 1-4 discloses that the GetNextKey algorithm is well-known in the art, as well as other hashing algorithms. Applicant also states that the use of smart cards for transaction is also well-known, inherently disclosing supporting smart card infrastructure such as, for example, communication between the smart and associated translational computers. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Muftic with the Applicant's own admission because Applicant's admissions are considered well-known to those of ordinary skill in the smart card arts.

Muftic and Applicant do not specifically disclose that customer data contained within smart card memory is hashed with a specific key unique and known only to the smart card

and the issuing authority. Rankl, however, in an analogous teaching clearly discloses hashing consumer data with the smart card unique key (see at least section 4.3 and Figure 4.23). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Muftic/Applicant with Rankl because using a secret key (master key) to hash data provides non-repudiation and a high level of security during the transaction.

In addition, Muftic does disclose providing a token or certificate (i.e. "master key") assigned to a unique client account (see citations used in claims 1, 8, 11) and the authorization process performed at a credit card issuer or bank (Fig 13, associated text) using well-known methods for authenticating a client, merchant, and transaction to be authorized. Muftic also discloses that when using hashes, the method for determining if a message is authentic is by doing a similar hash and comparing the results (C2, L27-37). Therefore, it would have been obvious to one ordinarily skilled in the art at the time the invention was made that in order to perform a proper validation and authorization of a transaction, the authorizing entity must inherently perform a parallel hashing of merchant, client, transaction IDs, and matching master key, and then compare the resulting digest with the one received from a requestor, in order to determine whether the request may be authorized.

Moreover, Muftic clearly teaches that the way to authenticate a hashed message is by using the same components, doing a parallel hash, and comparing the results. Therefore it would have been obvious to one ordinarily skilled in the art at the time the invention was made to include these steps in the authentication of authorization requests, so that proper validation and authentication may be done.

Claim 2:

Muftic discloses all the limitations of claim 1. Muftic further discloses *the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information* (see at least Fig 16: "seller's ID").

Claims 3, 14, 25, 26, and 33:

Muftic discloses all the limitations of claims 1, 13, 24, 32. Muftic does not specifically recite that *the request includes unique merchant information which is used to access the master key*. However, Muftic teaches that merchants also need to have specific accounts with credit card issuers in order to obtain credit for the transactions they enter into with clients (Fig 16: steps 1610, 1620). It is also inherent in the art that all merchants wishing to participate in an electronic commerce system need to establish accounts in advance with banks, credit card issues, clearing houses, and the like. Therefore it would have been obvious to one ordinarily skilled in the art at the time the invention was made to ensure that a request for billing digest would include unique merchant information that would dictate which master key the client system will fetch (i.e. Visa, MasterCard, AMEX, etc.). This would be inherent in the system, in order to allow it to properly match account holders and financial institutions.

Claim 5:

Muftic discloses all the limitations of claim 1. Muftic further discloses *creating the digest by hashing is performed by a smart card* (see at least C4, L33-43; Fig 3, associated text).

Claim 7:

Muftic discloses all the limitations of claim 1. Muftic further discloses *the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, the unique requestor information includes information describing a merchant identifier which is*

specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client (see at least Fig 13, associated text).

Claims 8, 11, 13, 20-24, 32, 39, and 40:

Independent claims 8, 11, 13, 20-24, 32, 39, and 40 recite essentially the same limitations as independent claim 1, nearly identical in scope and intent, and are therefore rejected on the same grounds as clearly disclosed in the rejection of claim 1 above.

Claim 12:

Muftic discloses all the limitations of claim 11. Muftic further discloses *receiving a response from the credit card issuer* (see at least Fig 13, associated text).

Claims 17, 28, and 36:

Muftic discloses all the limitations of claims 13, 24, 32. Muftic further discloses *creating the digest by hashing is performed by a smart card* (see at least C4, L33-43; Fig 3, associated text).

Claims 6, 10, 18, 29, and 37:

Muftic discloses all the limitations of claims 1, 8, 13, 24, 32. Muftic further discloses that encryption will be used in his system (C7, L1-15). Muftic does not specifically recite *encrypting/decrypting the unique client information, prior to retrieving the unique client information.* However it would be obvious to one ordinarily skilled in the art at the time the invention was made that all unique client information (i.e. certificates, signatures) would need to be kept secure to prevent unauthorized access or capture. Therefore it would just be common sense to encrypt this client information before retrieving it and transmitting it to a vendor.

Claims 19, 30, and 38:

Muftic discloses all the limitations of claims 13, 24, 32. Muftic further discloses *the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, the unique requestor information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client* (see at least Fig 13, associated text).

Claim 31:

Muftic discloses all the limitations of claim 24. Muftic further discloses *using a biometric for enhanced security of his system* (see at least C16, L41-51).

9. Claims 4, 9, 15-16, 27, and 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic/Applicant/Rankl in view of Nguyen et al., (US Patent 5,931,917).

Claims 4, 9, 15-16, 27, and 34-35:

Muftic/Applicant/Rankl discloses all the limitations of claims 1, 8, 13, 24, 32. Muftic/Applicant/Rankl does not specifically disclose *using reference numbers and checking to see if old references numbers have already been used when authorizing requests for transaction authorizations.* Nguyen, however, discloses the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party (see at least C26, L19; C28, L17; C29, L57; C37, L25). It would have been obvious to one ordinarily skilled in the art at the time the invention was made to add reference numbers to the client information as taught by Nguyen, in order to further be capable to prevent fraudulent transactions because each transaction authorized by the

issuer may be assigned a new reference number, thereby preventing the authorization of multiple requests for the same transaction.

Conclusion

10. **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

11. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **James A. Reagan** whose telephone number is **(703) 306-9131**. The examiner can normally be reached on Monday-Friday, 9:30am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **James Trammell** can be reached at (703) 305-9768.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the **Receptionist** whose telephone number is **(703) 305-3900.** Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(703) 305-7687 [Official communications; including

After Final communications labeled "Box AF"]

(703) 308-1396 [Informal/Draft communications, labeled "PROPOSED"

or "DRAFT"]

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, 7th floor receptionist.

JAR

08 March 2005